Complex & Intelligent Systems (2021) 7:2157–2177
https://doi.org/10.1007/s40747-021-00409-7

SURVEY AND STATE OF THE ART

Online social networks security and privacy: comprehensive review and analysis

Ankit Kumar Jain[1] · Somya Ranjan Sahoo[2] · Jyoti Kaubiyal[1]

Received: 1 March 2021 / Accepted: 19 May 2021 / Published online: 1 June 2021
© The Author(s) 2021

Abstract
With fast-growing technology, online social networks (OSNs) have exploded in popularity over the past few years. The pivotal reason behind this phenomenon happens to be the ability of OSNs to provide a platform for users to connect with their family, friends, and colleagues. The information shared in social network and media spreads very fast, almost instantaneously which makes it attractive for attackers to gain information. Secrecy and surety of OSNs need to be inquired from various positions. There are numerous security and privacy issues related to the user's shared information especially when a user uploads personal content such as photos, videos, and audios. The attacker can maliciously use shared information for illegitimate purposes. The risks are even higher if children are targeted. To address these issues, this paper presents a thorough review of different security and privacy threats and existing solutions that can provide security to social network users. We have also discussed OSN attacks on various OSN web applications by citing some statistics reports. In addition to this, we have discussed numerous defensive approaches to OSN security. Finally, this survey discusses open issues, challenges, and relevant security guidelines to achieve trustworthiness in online social networks.

Keywords Online social network · Security and privacy · Social threats · Cyberbullying · Cyber grooming

Introduction

When the internet became popular in the mid-1990's it made it possible to share information in ways that were never possible before. But a personal aspect was still lacking in sharing information [1]. And then in the early 2000s, social networking sites introduce a personal flavor to online information sharing which was embraced by the masses [2]. Social networking is the practice of expanding one's contact with other individuals mostly through social media sites like Facebook, Twitter, Instagram, LinkedIn and many more [3]. It can be used for both personal and business reasons [4]. It brings people together to talk, share ideas and interests and make new friends. Basically, it helps people from different geographical regions to collaborate [5]. Social networking platforms have always been found to be easy to use. This is the reason social media sites are growing exponentially in popularity and numbers. Figure 1 shows the basic constituents of social networks and the fields in which it is playing a major role [6]. As the figure shows, social networking can be used for entertainment, building business opportunities, making a career, improving one's social skills, and forging relationships with other individuals [7]. Facebook and Myspace are among the most preferred social networking sites Since a large chunk of the online population utilize social media platform, it has become a significant medium to promote business, awareness campaign.

Since people consider social media as a personal communication tool, the importance to safeguard their information stored in these social networking sites is often taken for granted. With the passage of time, people are putting more and more information in different forms on social networks which can lead to unprecedented access to people's and business information. The amount of information stored in social networks is very enticing for adversaries whose aim is to harm someone. They can create havoc worldwide with this huge amount of information in hands. Moreover, social media has become a great medium of advertisement for marketers and if they do not take social media security

✉ Ankit Kumar Jain
ankit.jain2407@gmail.com

[1] National Institute of Technology Kurukshetra, Kurukshetra, India

[2] Vellore Institute of Technology Andhra Pradesh, Amaravati, India

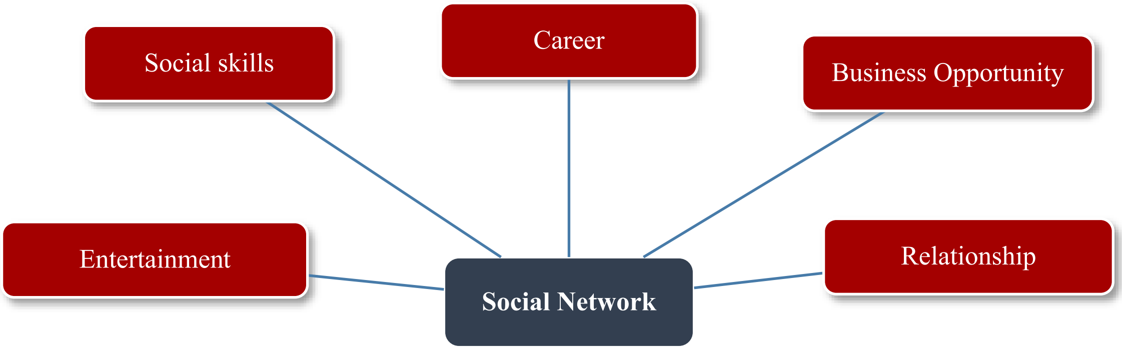


Fig. 1 Constituents of online social networks

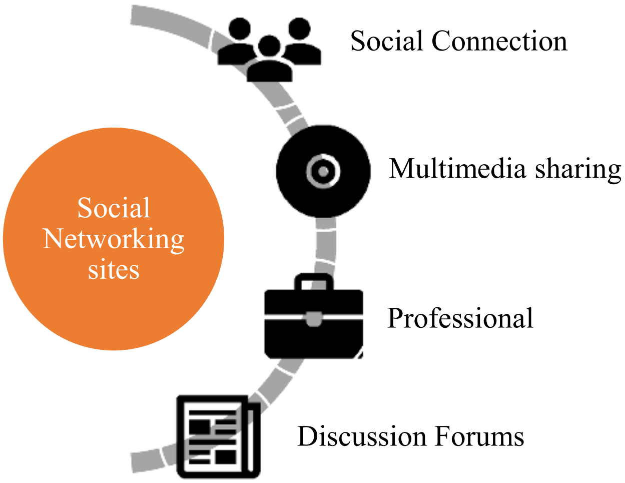


Fig. 2 Types of social networking sites

issues seriously enough, they make themselves vulnerable to a wide variety of threats and put their confidential data at risk. Also, social network can be classified into many types based on their uses. Social networks can be classified into four broad classifications namely, 'social connections', 'multimedia sharing', 'professional' and 'discussion forums'. This section discusses the types of social networking sites and vulnerabilities and instances of phishing that have occurred on said classifications. Current problems are also stated with an emphasis on malicious content-based phishing attacks. Figure 2 shows different types of social networking sites can broadly be classified into.

In Social connection, People use this network to connect with people and brands online. Although there are other types of social networking sites available online, this type certainly defines social media now. Sites that come under this category are 'Facebook', 'Twitter', 'Google + ', 'Myspace'. Although there are advantages of using these sites, it has some disadvantages also. These sites are vulnerable to phishing attacks in numerous ways. An intruder can make a portal that looks identical to a Facebook page. And then may lure users into entering into their credentials in different ways. Some of these methods are:

(a) Sending fake messages which states that their Facebook account is about to be disabled in a few days.
(b) The user may be tricked into clicking a link from the personal message sent by his friend stating that someone has uploaded personal pictures of the user in the given link.
(c) Some attackers send a message claiming that the user's account needs to be updated to use it further. And a link is given to download that update which contains an address of the malicious site.

Also, multimedia sharing networks are used to share pictures, videos, live videos, and other media online. They give an opportunity to users and brands to share their media online. Sites under this category are 'YouTube', 'Flickr', 'Instagram', 'Snapchat'. Nowadays every social media has an "inbox" feature where anyone can send messages to their friends and chat with them. Recently, YouTube has also released this feature. This gives the attacker a great opportunity to phish his target. He can send a shortened URL in the message which redirects the user to a malicious website [8]. Since it is not easy to recognize a shortened URL, whether it is legitimate or not, attackers take advantage and obfuscate their malicious content in shortened URLs. Professional social networks are developed to provide career opportunities to their users. It may provide a general forum or may be focused on specific occupations or interest depending on the nature of the website. 'LinkedIn', 'Classroom2.0', 'Pinterest' are some of the examples of professional social networking sites. Since these social networking sites contain all professional information of the user including email id, an attacker can use these details to send a victim a personalized mail. These emails may be like emails claiming prize-money which contains the malicious link. Similarly, in discussion forums, people use these networks to discuss topics and share opinions. These networks are an excellent resource for market research and one of the oldest forms of social network. 'Reddit', 'Quora' and 'Digg' are some examples of popular discussion forums. In these forums, people also share links related to their research so that users can get more information about their topic of research. Some illegitimate users share malicious links to lead astray users to some phishing websites. In this way, phishing can also be done in discussion forums.

The lasting part of our paper is incorporated as follows. We present different statistics for OSN security in "Statistics of online social network and media" section. Segment 3 particularizes the positive and negative impacts of online social networking. In Segment 4, we depict different threats that affect the user behavior in OSN platform. We describe the reason behind the OSN security issues in-depth in Segment 5. In "Solutions for various threats" section, we discuss the defensive solutions for various threats. For user awareness in "Security-guidelines for OSNs user" section, we portray certain security rules to protect your system, account, and information. In the following section, i.e. in "Open research issues and challenges" section, we portray the open research issues and challenges for OSN users. At last, we conclude our work in "Conclusion" section.

Statistics of online social network and media

Near about 4 billion users exist in the online internet landscape [9]. Out of the total population on the internet, there are 2.7 billion monthly dynamic clients on Facebook, 330 million active users on Twitter, 320 million active users on Pinterest, as of Dec 30, 2020 [10]. Figure 3 illustrates the number of users on different social networking platforms [11]. According to a report from Zephoria, there is a 16 percent increase year over year in monthly active users of Facebook. Seven new profiles are created every second [12]. Users uploaded a total 350 million pictures per day. On average 510,000 comments are posted in every 60 s on Facebook, 298,000 statuses are updated, and 136,000 photos are uploaded. Since a huge amount of data is uploaded on Facebook, there is a high chance of having security risks. Anyone can post malicious content hidden inside multimedia data or with shortened uniform resource locators (URLs). There are around 83 million fake profiles which can be of illegitimate users or of professionals doing testing and research. Around 1 lakh websites are hacked daily [13].

As per the data depicted in Fig. 4, the use of social networking sites has amplified exponentially such that there is a large amount of data and information available on these sites which has increased risks of information leakage and has opened doors for several cyber-crimes like data interception, privacy spying, copyright infringement, and information fraudulence. Although some Social Networking Sites like Twitter do not allow disclosing private information to users, some experienced attackers can infer confidential information by analyzing user's posts and the information they share online. The personal information we share online could give cybercriminals enough to get our email and passwords. We have taken cognizance of popularity and narrowed down the list of networks to keep the scope of study feasible. By extension, the chosen social networks employ state-of-the-art defence strategies. Thus, any possible attacks on these networks would employ state-of-the-art techniques. Transitively, the analysis holds relevance for other social networks as well.

Insights in Fig. 5 presents a positioning of the most banned sorts of hacking. It is as indicated by the reaction of adults to a survey in the United States during January 2021. It reports around 44% of the respondents accept that digital secret activities ought to have the most severe punishments.

Fig. 3 Number of users on different social networking platforms

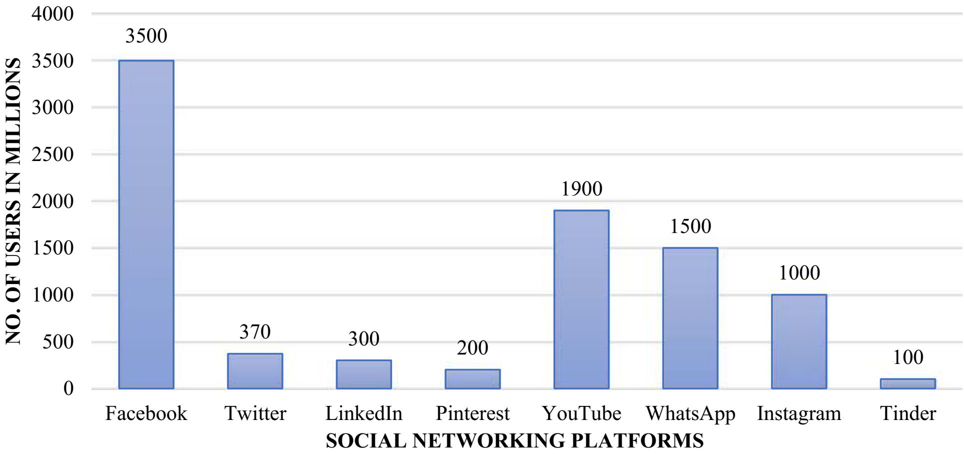


Figure 6 portrays the most vulnerable way for information breaches worldwide in 2021, sorted by share of identities exposed [14]. According to the recent report, 91.6 percent of data breaches resulted in impersonation or stolen identities.

Nowadays geotagged photos are very popular. People tag their geographical locations along with their pictures and share them online. Some applications have this feature of geotagging which automatically tags the current location inside a picture until and unless the user turns it off manually. This can expose one’s personal information like where one lives, where one is traveling, and invites thieves who can target one for robbery. When someone updates their status with their whereabouts on a regular basis, it can pose a threat to their life through possible stalking and robbery. According to a report by Heimdal Security, around 6 lakh Facebook accounts are hacked daily [15]. Individuals who

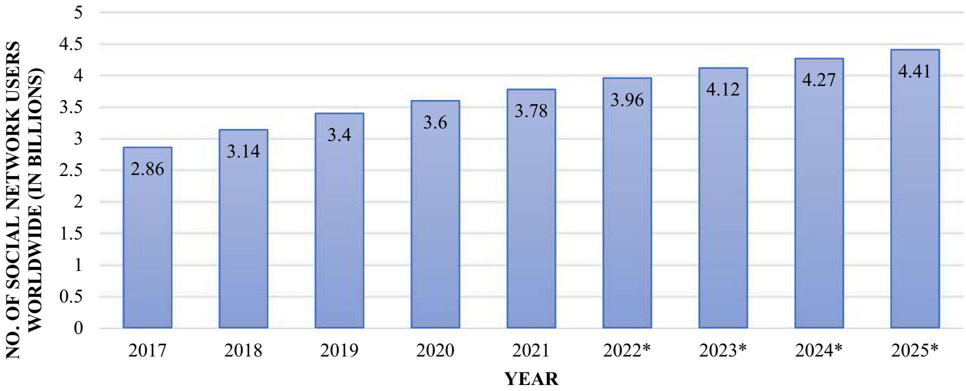


Fig. 4 Number of users on social media worldwide (year-wise)

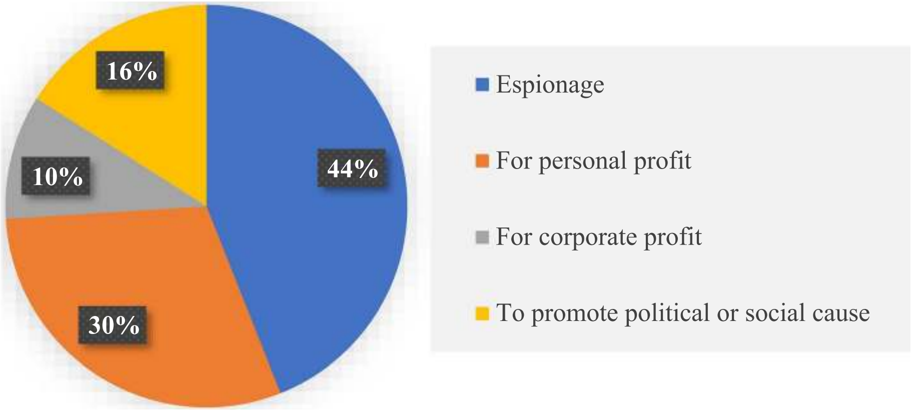


Fig. 5 Most punishable types of hacking in 2021

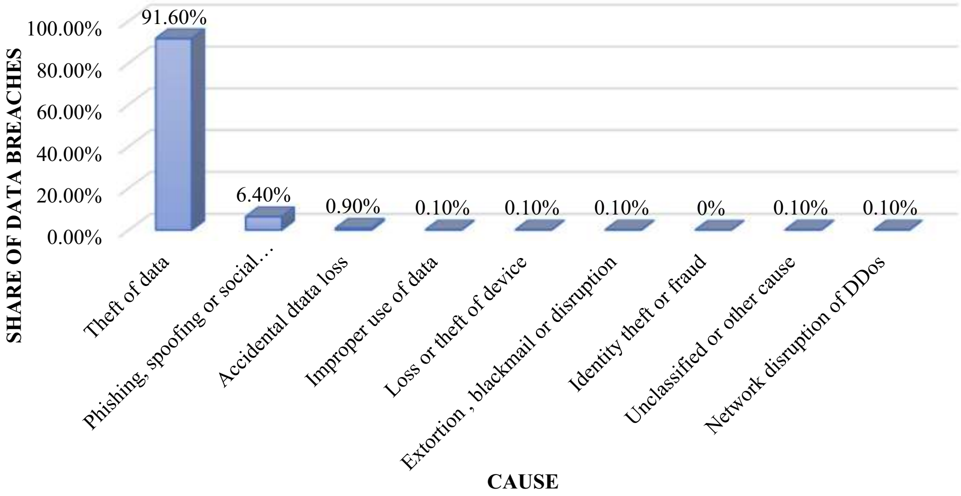


Fig. 6 Leading cause of data breaches worldwide in 2020

devote more time on social media and are probable to like the posts of their close friends. The hackers take advantage of this trust. Hackers can also use social media to sway elections. The most popular attacks on social media are likejacking, which occurs when attackers post fake Facebook like buttons to web pages, phishing sites, and spam emails. The statistics in Table 1 entail the percentage of internet users in the United States who have shared their passwords on their online accounts and to their loved ones as of May 2020. It is sorted by age group. The entire survey depicted that 74% of respondents aged more than 65 and above do not share online passwords with family and friends.

With this remarkable expansion in social networking threats and security issues, numerous specialists and security associations have proposed different solutions for alleviating them. Such solutions incorporate PhishAri for phishing detection [16], spam detection [17], GARS for cyber grooming detection [18], clickjacking detection system [19], framework to detect cyber espionage [20], SybilTrap to detect Sybil attacks [21], worm detection system to detect malware [22]. Users themselves must be alert while posting any media or information on social networking sites. A strong password should be adopted, and it must not be shared with anyone. One should check the URL while visiting a website and must not click any malicious links. These habits could help a user to some extent to be protected against various cyber-attacks on social media. Table 2 presents a collection of the greatest online information breaks via social media worldwide as of November 2020 [23].

Table 1 Percentage of users in the US who have shared passwords online with family or friends in 2020

Age group	Have shared (%)	Have not shared (%)
All adults	42	58
18–30	55	45
31–50	42	58
51–64	37	63
65 +	26	74

Positive and negative effects of online social networks based on users perspective

Social media has changed the manner in which individuals see the world and collaborate with each other. The near-universal accessibility and minimal effort of long-range informal communication locales, for example, Facebook and Twitter have assisted millions to stay connected with family and friends [28]. Similar to many technological revolutions, social networks also have a negative side. We describe some of the positive and negative effects of social networking based on the researchers' perceptions described below.

Positive factors of OSN

The various positive factors that influence the user to create and use the environments are maintaining social relationship, marketing the product and platforms, rescue efforts, and finding common group of people to communicate and share the thoughts.

(1) *Maintaining social relationships* Social networking sites have proven to be convenient in keeping up with the lives of others who matter to us. It helps to nurture friendship and other social relationships [29].

(2) *Marketing platform* Professionals can post work experience and build a network of professionally oriented people on sites such as LinkedIn or Plaxo which are career-building social networks [30]. They help discover better job opportunities. Marketers can influence their audience by posting advertisements on social networking sites [31].

(3) *Rescue efforts* Social media sites play a huge role in rescue and recovery efforts during calamities and disasters [32]. They connect people during such crucial times when the conventional societal structure has bro-

Table 2 Biggest data breaches on online social networks as of 2020

Platform	Year	Records stolen	Description
Facebook	April 2020	87 million	A large number of profiles of US residents were gained, and the information was utilized to construct a software program to foresee and impact electors [24]
MySpace	May 2018	427 million	An online hacker team made available an enormous set of stolen MySpace username and password combinations for sale [25]
Friend Finder Network Inc	October 2016	412 million	Hackers were able to access the information of hacked accounts of all the social sites and leak the information over the internet [26]
LinkedIn	June 2014	117 million	A Russian hacker sold 117 million email and password blends on a dark web marketplace and found guilty [27]

ken down. Bulletins are easily managed by social networking sites which can reunite missing family members. The public can be kept informed using utilities extended by essential service providers through online social networking. Real-time local updates on social media help government officials to better understand the circumstances and make more informed decisions.

(4) *Finding common groups* Social networking sites help people find groups with common interest [33]. People can share their likes and dislikes, interests and obsessions and thought and views to these groups which contribute to an open society.

Negative factors of OSN

When the general users use the social network platform, he/she face a lot of trouble that identified by various researchers based on security parameter. Like,

(1) *Online intimidation:* while making friends is easier on social media, predators can also find victims easily [34]. The anonymity provided by social networks has been a consistent issue for social media users. Earlier someone was bullied only face-to-face [35]. Nonetheless, now any individual can bully someone online anonymously.

(2) *The exploitation of private information:* although creating an account on social networking sites is free of charge, they make their money mostly from the advertisements they show on their websites [36]. The data once gathered is sold to brokers in relationships without the consent of social media users. Moreover, adversaries can also extract confidential information about their targets from these websites using different attack techniques.

(3) *Isolation*: social media has surely improved the connection between users but conversely it has also averted real-life social interaction [37]. People find it easier to follow the posted comments of people they know rather than personally visit or call them [38].

(4) *General addiction:* by the records we can depict that social media is more addictive than cigarettes and alcohol. People often feel empty and depressed if they do not check their social media account for a full day.

This paper presents a systematic and in-depth study of threats and security issues that are current and are emerging. More precisely, this study encompasses all the conventional threats that affect the majority of the clients in social networks and most of the modern threats that are prevalent nowadays with an emphasis on teenagers and children. The principle objective of this paper is to give knowledge into the social network's security and protection. It introduces the reader to all the possible dimensions of online social networks and issues related to them. Our analysis throws light on the prevalent open challenges and issues that need to be discussed to enhance the trustworthiness of online social networks.

The remaining paper is systematized as: "Statistics of online social network and media" section describes various threats that are currently prevalent in social media. "Positive and negative effects of online social networks based on users perspective" section provides reasons for social media security issues. "Various threats on online social network and media" section discusses solutions that are given by various researchers, "Reasons behind online social media security issues" section consists of some security- guidelines suggested for users, some open issues and challenges in online social media is conferred in "Solutions for various threats" section, finally, Segment 7 presents the conclusion.

Various threats on online social network and media

Being the technology-based society that we are, and with the prevalence of the internet, we have extended our interaction through the electronic world of the internet. Following are the attacks which users have been observing right from the beginning of social networks.

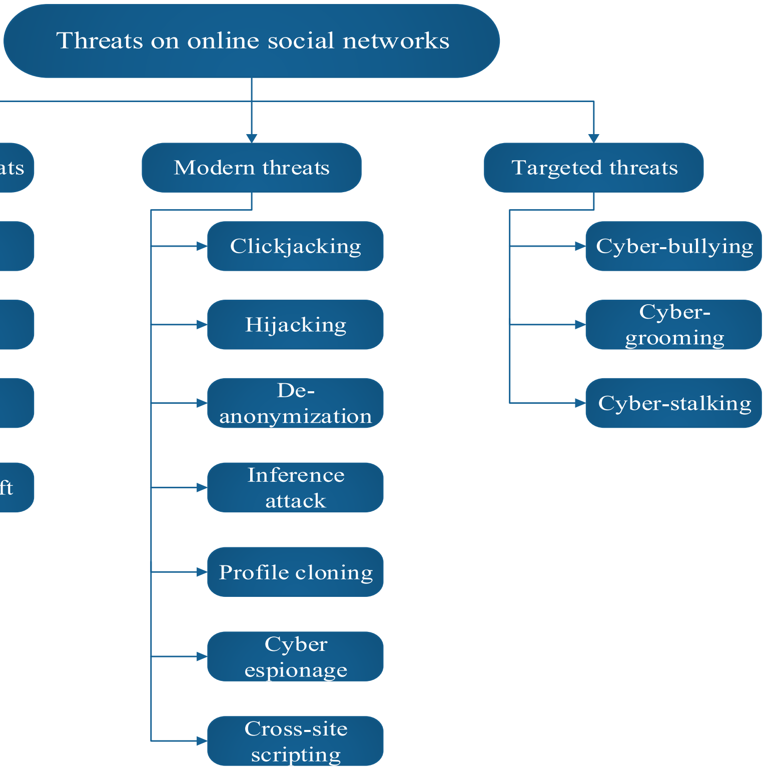
We have divided threats into three categories i.e. conventional threats, modern threats, and targeted threats (as shown in Fig. 7). Conventional threats include threats that users have been experiencing from the beginning of the social network. Modern threats are attacks that use advanced techniques to compromise accounts of users and targeted attacks are attacks that are targeted on some particular user which can be committed by any user for varied personal vendettas.

Conventional threats

Spam attack

Spam is the term used for unsolicited bulk electronic messages [39]. Although email is the conventional way to spread spam, social networking platform is more successful in spreading spam [40]. The communication details of legitimate users can easily be obtained from company websites, blogs, and newsgroup [27]. It is not difficult to convince the targeted client to read spam messages and trust it to be protected [41]. Most of the spams are commercial advertisements but they can also be used to collect sensitive information from users or may contain viruses, malware or scams [28].

Fig. 7 Classification of threats



Malware attack

Malware is a noxious programming which is explicitly evolved to contaminate or access a computer system, ordinarily without the information of the user [42]. An intruder can utilize numerous ways to spread malware and contaminate devices and networks [43]. For instance, malware may get installed by clicking a malicious URL, on the client's framework or it might divert the client to a phony site which endeavors to acquire private data from the client. An attacker can inject some malicious script in URLs and clicking on that URLs can make that script run on a system that may collect sensitive information from that system [44]. In social networking platforms, the malware uses Online Social Network's (OSN) structure to propagate itself such as the number of vertices, number of edges, average shortest path, and longest path.

Phishing

A phishing attack is a kind of social engineering attack where the aggressor can acquire sensitive and confidential information like username, password and credit card details of a user through fake websites and emails which appears to be real [45]. An invader can impersonate an authentic user and may use his/her identity to send fake messages to other users via a social networking platform which contains malicious URL [46]. That URL might readdress a consumer to the phony website where it asks for personal information [47]. In the case of SNS, an assailant needs to attract the client to a phony page where he can execute a phishing attack. To accomplish this, the assailant uses different social engineering methodologies. For example, he can send a message to a user which says, "your personal pictures are shared on this website, please check!". By clicking on that URL, the user is redirected to a fake website which looks like some legitimate social networking site.

Identity theft

In this sort of assault, the assailant utilizes someone else's identity like social security number, mobile, number, and address, without their permission to commit attackers [48]. With the help of these details, the attacker can easily gain access to a victim's friend list and demand confidential information from them using different social engineering techniques [49]. Since the attacker impersonates a legitimate user, he can utilize that profile in any conceivable way which could seriously affect authentic clients [50].

Modern threats

Cross-site scripting attack

Cross-site scripting is a very prevalent attack vector among infiltrators. The attack is abbreviated as XSS and is also known as “Self-XSS” [51]. Fundamentally, the attack executes a malicious JavaScript on the victim’s browser through different techniques. These are classified as persistent, reflected, and DOM-based XSS attacks [52]. The browser can be hijacked with just a single click of a button which may send a malicious script to the server [53]. This script is boomeranged back to the victim and gets executed on the browser. Attractive links and buttons in popular social media sites like Twitter and Facebook can trick the user into following URLs [54]. Worse yet, some users may feel compelled to copy and paste JavaScript containing links onto their browser’s address bar [55]. These attacks can either steal information or act as spyware. Such attacks can also hijack computers to launch attacks on unsuspecting users. The real perpetrator of the attack is hidden behind the compromised machine.

Profile cloning attack

In this attack, the assaulter clones the users’ profile about which he has a prior knowledge. The attacker can use this cloned profile either in the same or in a different social networking platform to create a trusting relationship with the real user’s friends [56]. Once the connection is established, the attacker tricks the victim’s friends to believe in the validity of the fake profile and catch confidential information successfully which is not shared in their public profiles. This attack can also be used to commit other types of cybercrimes like cyberbullying, cyber-stalking, and blackmailing [45].

Hijacking

In hijacking, the adversary compromises or takes control of a user’s account to carry out online frauds [57]. The sites without multifactor authentication and accounts with weak passwords are more vulnerable to hijacking as passwords can be obtained through phishing [58]. If we do not have multifactor authentication, then we lack a secondary line of defense [59]. Once an account is hijacked, the hijacker can send messages, share the malicious link, and can change the account information which could harm the reputation of the user [60].

Inference attack

Inference attack infers a handler’s confidential information which the user may not want to disclose, through other statistics that is put out by the user on some Social Networking Site (SNS) [61]. It uses data mining procedures on visibly available data like the user’s friend list and network topology [62]. Using this technique, an attacker can find an organization’s secret information or a user’s geographical and educational information [45].

Sybil attack

In Sybil attack, a node claims multiple identities in a network [63]. It can be harmful to social networking platforms as they contain a huge number of users who are coupled through a peer-to-peer network [64]. Peers are the computer frameworks which are associated with one another by means of the internet and they can share records straightforwardly without the need of a central server [32]. One online entity can make several fake identities and use those identities to distribute junk information, malware or even affect the reputation and popularity of an organization. For instance, a web survey can be manipulated utilizing various Internet Protocol (IP) delivers to submit an enormous number of votes, and aggressor can outvote a genuine client [33].

Clickjacking

Clickjacking is a procedure in which the invader deceives a user to click on a page that is different from what he intended to click [65]. It is also known as User Interface redress attack. The attacker exploits the vulnerability of the browsers to perform this attack [66]. He loads another page over the page which the user wants to access, as a transparent layer [67]. The two known variations of clickjacking are likejacking and cursorjacking. The front layer shows the substance with which the client can be baited. At the point when the client taps on that content he actually taps the like button. The more individuals like the post, the more it spreads.

In cursorjacking attacker replaces the actual cursor with a custom cursor image. The actual cursor is shifted from its actual mouse position. In this manner, the intruder can trick a consumer to click on the malicious site with clever positioning of page elements [68].

De-anonymization attack

In quite a lot of social networking sites like Twitter and Facebook, users can hide or protect their real identity before releasing any data by using an alias or fabricated name [69]. But if a third party wants to find out the real identity of the user, it can be done by simply linking the information leaked by these social networking sites [70]. They use strategies such as tracking cookies, network topologies, and user group enrollment to uncover the client’s genuine identity [71]. It is a sort of information mining method in which mysterious information is cross-referred to other information sources to re-recognize the unknown information [60]. An attacker can collect information about the group membership of a user by stealing history from their browser and by combining this history with the data collected. Thus the attacker can de-anonymize the user who visits that attacker's website [72].

Cyber espionage

Cyber espionage is an act that uses cyber capabilities to gather sensitive information or intellectual property with the intention of communicating it to opposing parties [73]. These attacks are motivated by greed for monetary benefits and are popularly used as an integral part of military activity or as a demonstration of illegal intimidation [74]. It might bring about a loss of competitive advantage, materials, information, foundation or death toll. A social engineer can perform social engineering assaults using social networking sites. He can acquire important data like worker's assignment, email address, and so forth utilizing social networking sites [75].

Targeted threats

Cyberbullying

Cyberbullying is the use of electronic media such as emails, chats, phone conversations, and online social networks to bully or harass a person [76]. Unlike traditional bullying, cyberbullying is a continuous process [77]. It is continuously maintained through social media [78]. The attacker repeatedly sends intimidating messages, sexual remarks, posts rumors, and sometimes publishes embarrassing pictures or videos to harass a person [79]. He can also publish personal or private information about the victim causing embarrassment or humiliation. Cyberbullying can also happen accidentally. It is very difficult to find out the tone of the sender over text messages, instant messages, and emails. But the repeated patterns of such emails, texts, and online posts are rarely accidental [80].

Cyber grooming

Cyber grooming is establishing an intimate and emotional relationship with the victim (usually children and adolescents) with the intention of compelling sexual abuse [81]. The principle point of cyber grooming is to acquire the trust of the youngster and through which intimate and individual information can be attained from the child [82]. The data is often voluptuous in nature through sexual conversations, pictures, and videos which gives the attacker an advantage to threaten and blackmail the child [83]. Assailants frequently approach teenagers or kids through counterfeit identity in child-friendly sites, leaving them vulnerable and uninformed of the fact that they have been drawn closer with the end goal of cyber grooming. However, the victim can also unknowingly initiate the grooming process when they get rewarding offers, for example, cash in return for contact details or personal photographs of themselves. In some cases, the victim knows about the fact that he/she is conversing with an adult which can prompt further commitment in sexual activities. However, it is with the individual under the age of consent and in this manner constitutes a crime. The anonymity and accessibility of advanced media permit groomers to move toward various youngsters simultaneously, exponentially increasing the instances of cyber grooming. Despite what might be expected, there are a couple of instances of feelings for the crime of cyber grooming worldwide, as 66% of the world's nations have no particular laws with respect to cyber grooming of children [84].

Cyberstalking

Cyberstalking is the observing of an individual by the means of internet, email or some other type of electronic correspondence that outcomes in fear of violence and interferes with the mental peace of that individual [85]. It involves the invasion of a person's right to privacy. The attacker tracks the personal or confidential information of the victims and uses it to threaten them by continuous and persistent messages throughout the day. This conduct makes the victim exceptionally worried for his own safety and actuates a type of trouble, fear or disturbance in him [86]. Most of the individuals these days share their personal information like telephone number, place of residence, area, and schedule in their social networking profile. In addition, they likewise share their location-based data. An assailant can gather this data and use it for cyberstalking [87].

Reasons behind online social media security issues

Social media addresses one of the most unique, unstructured, and unregulated datasets anyplace in the advanced world and this scene is arising quickly all over the globe [88]. Every day millions of people upload their photos and other multimedia content on social media to share it with their friends. This is prompting the development of digital risk monitoring [89]. The development of web-based media has presented new security standards that put clients (representatives, clients, and partners) solidly in the aggressor's line of sight. The social network has become the new digital milestone where attackers think that it's simple to target victims. It has presented one of the biggest, most powerful dangers to authoritative security. Attackers influence social media for the accompanying three reasons (as shown in Fig. 8):

(a) *The scale of social media:* since a huge mass of people spend their time on social media for various pur-

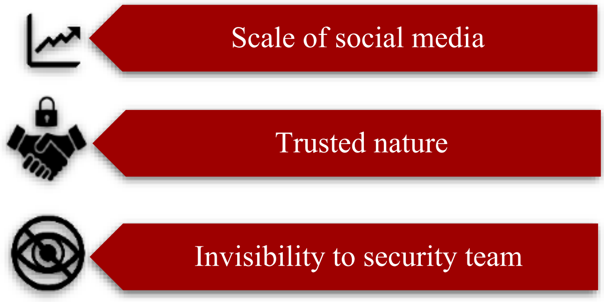


Fig. 8 Reasons for social media security issues

poses, attacks can spread like any other viral trend. The attacker can use hashtags, clickbait, and trending topics to announce their malware which might be focused on everyone or to some particular gathering of individuals. This represents a tremendous challenge for security experts to overcome physically.

(b) *Trusted nature of social media:* adversaries take advantage of the trusting nature of social media. People sometimes accept an unknown friend request on the basis of mutual friends that requester has. They easily visit the link posted by their friends without thinking much about a possible security breach. Over one-third of the total population on social media acknowledge unknown friend requests, making online media perhaps the best mode for acquiring the trust of a target.

(c) *Invisibility to security team:* majority of people in the world spend most of their time on social media networks. Observing this enormous populace is extremely troublesome as security teams do not have tools to broaden their perceptibility beyond a specific border into the social media domain where employees are intensively vulnerable to be compromised.

Solutions for various threats

Many researchers in both academia and industries are constantly trying to find solutions for the aforementioned threats in social media. They have proposed many solutions and some approaches to combat these threats. This section provides a discussion on various methods and approaches proposed by different researchers on SNS security. We have classified solutions into two groups namely social network operator solutions and academic solutions. Figure 9 shows the classification.

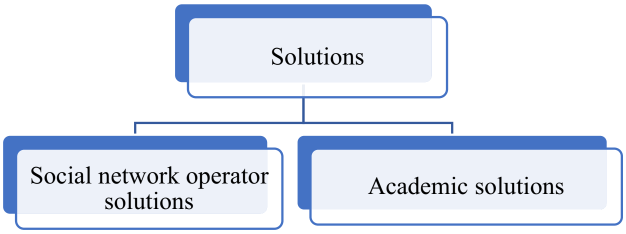


Fig. 9 Classification of solutions to threats

Social network operator solutions

Authentication mechanism

To make sure that only a legitimate user is logging or registering in a social network and not a socialbot, several OSN uses authentication procedures such as CAPTCHA, multi-factor authentication, and photos-of-friend identification. For instance, the leading social networks like Twitter and Facebook use two-factor authentication principles. This principle uses a login password and a verification code received through a mobile device. This helps to mitigate the risk of an account being compromised and prevents an attacker from hijacking a legitimate account and posting malicious content.

Security and privacy setting

Many social networking sites provide configurable security and privacy setting to empower the client to shield their personal information from undesirable access by outsiders or applications. For instance, the Facebook client can modify their security setting and select the audience (like friends, friends of friends, and everybody) in the network who can see their details, pictures, posts, and other sensitive information. Moreover, Facebook additionally permits its users to either acknowledge or reject the access of third-party applications to their personal information. Many social networking sites are equipped with security measures that are internal to the system. They ensure users of the network against spams, counterfeit profiles, spammers, and different risks.

Report users

Online social networks protect the young generation and teenagers from being harassed by providing the facility to report any form of abuse or policy violations by any user in their network. For instance, if a user sees something on Facebook that is objectionable to the individual's sentiments, but it doesn't violate the Facebook terms then the user can utilize the report links to send a message to the one who posted it asking him to take it down or remove.

When Facebook receives reports, it is reviewed and removed according to the Facebook community standards.

Academic research-based solutions

Phishing detection

Phishing distresses the privacy and security of many traditional web applications such as websites, social networking sites, emails, and blogs. Consequently, several anti-phishing techniques have been developed to detect phishing attacks. Many researchers have put forward anti-phishing procedures which are based on techniques that try to identify phishing websites and phishing URLs. As phishing attacks are becoming more and more pervasive in online social networking sites, the research community has suggested specialized solutions for phishing attacks in a social networking environment. For instance, Aggarwal et al. proposed the PhishAri technique for real-time identification of phishing attacks occurring on Twitter. It utilized specific Twitter features like account age and number of followers to detect if the posted tweet is phishing or safe [16].

Cyberbullying detection

Although detecting cyberbullying is more complex than detecting racist language and spam [90], some researchers have tried to detect it using more complex document representation and additional information about victims and bullies [91].

Machine learning techniques can be applied to detect cyberbullying [92]. Rather than using only words and emoticons which expresses insults, obscenity, and typical cyberbullying words [93], it can also use some additional information like the gender and personality of the participants in a suspected cyberbullying event [94]. To deal with uncertainty and imprecision, a fuzzy rule-based system can be used which is a mathematical tool. To optimize the results genetic algorithms are the direct and stochastic methods.

Cyber grooming

For addressing the problem of online cyber grooming, machine learning techniques appear to be an effective measure. Michalopoulos et al. [18] presented the Grooming Attack Recognition System (GARS) a technique to recognize, analyze and control grooming attacks so that children could be protected against online attacks. It calculates the total risk value which identifies grooming threats to which a child is exposed by analyzing conversations by the child. A threshold is predefined for risk value and when the total risk value crosses the predefined threshold, an alarm mechanism is prompted. This alarm mechanism also simultaneously transmits an on-the-spot warning message to the parent. A colored signal is generated to warn the child about the degree of danger in a conversation. Escalante et al. [95] evaluated the use and performance of a profile to detect sexual predators. Through this evaluation, they also investigated aggressive texting.

Clickjacking

Balduzzi et al. [19] designed and developed an automated system that can analyze web pages to protect the user against clickjacking attacks. It consists of a code that can detect overlapping clickable elements. And in addition to this solution, they also adopted the NoScript tool, which has an anti-clickjacking feature included in it. Anas et al. [96] proposed a solution in which other visual components are added which guarantees that the user is not able to proceed with his actions until and unless he has visibility over the control in place. To enable the working of this solution, the existence of a HyperText Markup Language (HTML) object containing a pattern was ensured. Some checkpoints are generated based on user interaction. User must follow those checkpoints without a single mouse click. In addition to it, a panel area shows the third-party reference identity. And to ensure the integrity of actions, user interface verification control is used. This technique can be applied in two ways, one is by generating random patterns in which the user has to follow that pattern to further propagate his action and the other way is to ask the user to draw that specific pattern which he has already registered. Microsoft introduced X-FRAME-OPTIONS, an Hyper Text Transfer Protocol (HTTP) header sent on HTTP responses, as a defense against frame busting and clickjacking in Internet Explorer 8. JavaScript can also be used as a defense against clickjacking [97].

Cyberstalking

Encryption techniques are available for devices on recent versions of Android and iOS. If a device is stolen, the thief cannot read the contents if encryption is enabled. Further, any attempts to read the information from internal or external memory is thwarted by the existence of a device password [98]. There are various technologies which can be used against stalkers like smartphone fingerprint lock antivirus, specialized stalker app detection software, firewalls, and privacy guards. Device encryption can be used against spyware, stalker apps and device theft [98]. Frommholz et al. have described machine learning techniques for detecting cyberstalking using textual analysis altogether [99].

Cyber espionage

Cyber espionage is a kind of targeted attack. Sahoo et al. described the concept of an ATA detection framework and introduced a system design checklist which is explicitly designed for identifying targeted attacks [20]. Organizations can create their own team to fight against targeted attacks and analyze vulnerabilities, in their and as well as in other companies' code. Google has its own team to analyze vulnerabilities and bugs in their code. Each company has its own profile that is different from each other. So, each company must take appropriate steps according to their profile to implement security measures to design and implement security controls to address various security risks. Organizations can also be secured to some extent against targeted attacks by means of authentication systems. Earlier only password was used to protect the data, but now a two-factor authentication system is used which is a combination of password and some pin or biometric details. It is more secure than using a single factor i.e. password. The data which is no longer required for business purposes should be removed from the company's network. Keeping those records may create the risk of unauthorized access to sensitive information in an organization [100].

Fake profile

The author in Ref. [101] describes one model to distinguish the counterfeit accounts and profiles. They extracted some user profile contents from LinkedIn platform and processed those profiles content to extract different features. Subsequent to preprocessing of profiles through principal component, a training set is created utilizing the resilient backpropagation algorithm in a neural network. Support Vector Machines (SVMs) is utilized for characterization of profile. The author in Ref. [102] proposed a model that detects bot net using adaptive multilayered-based machine learning approach. The proposed work presented a bot detection framework based on decision trees which effectively detects P2P botnets. Also, the author in Ref. [103] proposed an ensemble classification model for the detection of fake news that has achieved a better accuracy compared to the other state-of-the-art. The proposed model extracts important features from the fake news datasets, and the extracted features are then classified using the ensemble model comprising of three popular machine learning models namely, decision tree, random forest, and extra tree classifier. Furthermore, the author in Ref. [104] presented a systematic literature review of existing clone node detection schemes with some theoretical and analytical survey of the existing centralized and distributed schemes for the detection of clone nodes in static WSNs environment.

Sybil detection

Al-Qurishi et al. [105] proposed a new Sybil detection system that uses a deep learning model to predict a Sybil attack accurately. This model consists of three modules namely, one data harvesting module, one feature extracting module and a deep regression model. All these three modules work in a systematic form together to analyze a user's profile on Twitter. Rahman et al. gave a model named SybilTrap which is a graph-based semi-supervised learning system that uses both content-based and structure-based techniques to detect Sybil attacks. It is based on a semi-supervised algorithm which utilizes the interaction graph information of a node where labeled information of nodes flows through unlabeled nodes. It gathers information about the network and its users and uses this information to detect malicious users. This system is resistant to various strategic attacks such as targeted or random attacks. It is designed to work under any condition and is applicable to all existing social networks regardless of their level of trust [21].

Spam detection

Rathore et al. proposed a framework called SpamSpotter to solve the issue of spam attack on Facebook. It is based on the intelligent decision support system (IDSS). It gathers all relevant information from the user profile with the help of a decision process in IDSS and then analyzes it by mapping user data to the classification of a user profile as a spammer or legitimate. It resolves some of the issues and challenges (1) It solves the issue of an inadequate set of features that exist in most of spammer detection system. (2) It resolves the issue of uncertainty about critical pieces of Facebook information and public unavailability. (3) The use of the IDSS system resolves the issue of low accuracy and high response time. The use of machine learning classifiers in IDSS provides fast response time that is very essential to detecting spam on Facebook [17].

Malware

Faghani and Saidi [106] found that the visiting behavior of the social network members affects the propagation of XSS worms. The worm propagates slower when members mostly visit their friends rather than strangers. It can also be slowed down by the clustered nature of social networks. This is so because infected profiles in the early stages of XSS worm propagation lead to faster propagation of worm. Xu et al. [22] developed an approach to detect worms which leverages properties of online social network and propagation characteristics of OSN worms. It first builds a surveillance network based on the properties of the social graph to gather evidence against suspicious worm propagation. It monitors only a small fraction of user accounts to maximize surveillance coverage. To ensure that noise is absent in a surveillance network, a scheme is further proposed. Table 3 represents the probability of encountering different types of threats in different platforms discussed in "Introduction" section. It shows that the platforms used for social connections are the most vulnerable among all platforms.

Other contributions

The author in Ref. [107] proposed a novel algorithm to reform any traffic domain into a complex network using the principles of decentralized Social Internet of Things (SIoT). With the help of social networking, concepts integrate into the Internet of Things (IoT), the concept of SIoT has been proposed. The idea of the article is, every vehicle acts as a smart thing, communicate with nearby vehicles within a particular distance in a decentralized manner and together form a complex network. Also, the author in Ref. [108] proposed propose a privacy-preserving ICN forwarding scheme based on homomorphic encryption for wireless ad hoc networks to protect the private information of the user. The trust-based model proposed by the author in Ref. [109]. The author proposed a secure trusted hypothetical mathematical model for ensuring secure communication among devices by computing the individual trust of each node. In addition to this, the author proposed a decision-making model, that integrated with the hypothetical model for further speeding up the real-time communication decision within the network.

Comparative analysis with other state of art techniques

This section compared our survey related to different threat analysis and their defensive approaches with other state of art techniques and survey to show the novelty shows in Table 4.

Security-guidelines for OSNs user

Nowadays, online social media and network have become an integral part of everyone's life. As the reputation of these social sites grows, so do the risks of using them. The number of users increases exponentially every year. So, it becomes a necessity to secure users on these platforms. Below are some security-guidelines for users which they can practice keeping themselves reasonably secure. We have tried to give security-guidelines in two ways. First, it has been described in a general form and then it is described platform-wise (as shown in Fig. 10).

General guidelines

(a) *Use a strong password:* for maintaining the security of accounts, users should choose a strong password. It should not be too short as short passwords can be easily guessed. It should be long enough and must contain alphanumeric values with some special characters [119]. Users should not use the same password which they use for other accounts because if somehow an attacker gets to know that password, he can compromise all accounts of that user. So, choosing a strong password can help a user safeguard their account and profile from unauthorized access [120].

(b) *Limit location sharing:* nowadays sharing location has become a trend. Many social networking sites have also introduced the feature of geotagging which automatically tags the geographical location of the user when the user uploads any multimedia on social media [121].

Table 3 Probability of encountering different threats in different platforms

		Platforms			
S.N.	Possible threats	Social	Professional	Multimedia	Discussion forums
1	Spam	Medium	High	Low	Very low
2	Malware	High	Medium	Low	Low
3	Phishing	High	Medium	low	High
4	Identity theft	High	High	High	Low
5	Clickjacking	High	Low	Medium	Low
6	Hijacking	High	High	High	Low
7	De-anonymization	High	Medium	Low	Very low
8	Inference	High	Medium	Low	Low
9	Profile cloning	High	Medium	Medium	Very low
10	Cyber espionage	High	High	Medium	Medium
11	Cyber bullying	High	Low	High	Medium
12	Cyber grooming	High	Very low	High	Low
13	Cyber stalking	High	Low	High	low

Table 4 Comparison of our survey with other existing survey on online social networks

Author details	Different threats														
	Spear phishing	Fake profile attack	Graph-based attack	peculation attack	Online chat risk	Sybil attack	Friend in middle	Phishing attack	Spamming attack	Malware	OSN aggregator	Cross site request forgery	Cyber stalking	Cyber bullying	Corporate espionage
Pandey et al. [110]	√	√	√	√	√					√	√	√			√
Peng et al. [111]	√	√	√	√				√	√	√			√	√	√
Dakiche et al. [112]	√			√	√	√	√			√	√	√	√		
De Salve et al. [113]			√	√	√	√			√	√	√	√	√		√
Ramalingam and Chinnaiah [114]					√	√	√	√	√	√	√	√	√		
Sarmah et al. [115]			√	√				√	√	√			√	√	√
Song et al. [116]	√	√			√	√			√	√	√				√
Maleszka [117]	√			√	√	√		√	√			√	√	√	√
Tse et al. [118]	√	√		√			√	√	√		√	√			√
Our survey	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

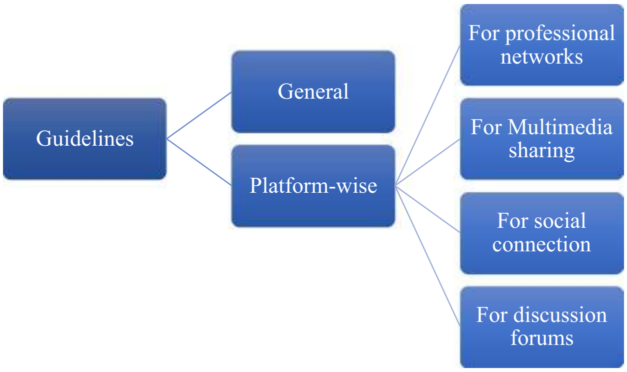


Fig. 10 Security guidelines for users

The user has to switch it to manual so that it does not tag location automatically. Sharing location online makes a user vulnerable to real-life crimes like robbery. So, to mitigate this risk, the user can post his location at a later point of time post completion of the visit [122]. Users must upload their multimedia content online very carefully as it may contain sensitive metadata and it is recommended to switch geotagging to manual mode in all their mobile devices and accounts. Also suggested is the use of software that removes such metadata from the pictures before uploading.

(c) *Be selective with friend requests:* it is seen that many users accept friend requests without analyzing the complete profile of the requester. People generally accept friend request based on mutual friends. If the requester has some mutual friends, then they accept it [123]. Sometimes attackers make their profile attractive deliberately or they may impersonate an account. So, if the person sending a friend request is unknown, one should ignore that friend request. It could be a fake account attempting to steal sensitive information.

(d) *Be careful about what you share:* users should be careful about their posts as it may reveal their personal information and sometimes others also. Many organizations keep strict rules and regulations for sharing information and multimedia content. There are many reports of people getting fired from their job due to sharing information illegally. This situation can be avoided if employees are well informed about the protocols of the organization they are working in regarding pictures, videos, and messages that they post online. Sharing information illegitimately can harm an organization's reputation in the market along with its data and intellectual property also.

(e) *Be aware of links and third-party applications:* illegitimate users can get access to someone's account and get sensitive information by sharing a malicious link. Nowadays shortened URLs are becoming very popular on various social media platforms. These shortened URLs may be obfuscated with malicious code or script. These scripts try to gather the personal and confidential information of a user which may breach the privacy of that user. Moreover, hackers may take advantage of vulnerabilities present in a third-party application that is integrated with many popular social networks [124]. An example of such a third-party application happens to be games that are playable on online social networks which ask for user's public information to consume their services. This gathered information may be provided to outsiders or third-party interventions. To avoid this risk, user should be careful while installing third-party applications in their profile.

(f) *Install internet security software:* some threats whose pattern is known may easily be detected through anti-viruses. Threats like cyber grooming, cyberbullying can be detected to some extent by using anti-virus software [125]. Many malicious links can be shared by our friends unknowingly which redirects the user to some phishing website. Anti-virus software should be kept updated regularly due to the presence of many viruses created by hackers on a daily basis. Some social networking sites also have their own security tools which can be used by users to protect themselves from cyber-attacks.

Platform-wise

For professional networks

(1) Professional networks are primarily used to create contacts and increase perceptibility to potential recruitment companies [126]. So, to be safe on professional networks, one should look for the details provided by other users before adding them to one's contact list. Generally, an adversary does not provide many details about his career.

(2) A user should check if there are any spelling or grammar mistakes in someone's profile because if someone is applying for some job, it should be very well written and should be free from any spelling or grammar mistakes [127]. It should contain good information about that person.

(3) Checking for consistency in a person's career can be a good practice if a user wants to be safe on a professional network. A profile which continually and definitely changes over a short span of time is the most used part as a draw by the invader. At the point when the fraudster needs to target one sort of organization or vertical, he simply adds a new position that could be pertinent to his targets.

(4) One should also cross-check information. If a person claims to be from the employer's company, the user can check the company's directory and should not hesitate to verify from his company's human resource department.

For multimedia sharing platform

(1) One should not post sensitive information in their photos or caption [3]. Exposing too much private information in a profile can be dangerous.
(2) Sharing current locations on social media should be avoided. Geotagging services provided by different multimedia platforms should be turned off manually. There have been plenty of cases of thieves that were tipped off to rob homes. Suspects use social media to gather information about victims who share their location online. People who leave for a short holiday and brag about it online may come home to find the place emptied.
(3) If an application is not in use for a long period, it is better to revoke access to that application. There are so many third-party applications which use social media account to log-in. For security and privacy concerns, one should allow access to applications that are trustworthy [4].
(4) Enable two-step authentication for all your social media accounts wherever possible. This provides an extra layer of security to the account. In case an adversary finds out the password of a user, he will still need a second factor to authenticate himself. The second factor consists of a unique, time-sensitive code that users receive via text on their mobile phone.

For social connection platform

(1) Users should learn about the privacy and security setting for different social media platforms and use them [128]. Each platform has its own privacy and security setting. Every platform provides settings, configuration, and privacy sections to limit who and what groups can see various aspects of the user's profile. The privacy setting provided by the sites as default should not be adopted as it is.
(2) The more details provided, the easier it is for an adversary to use that information to steal identity or to commit other cybercrimes. Thus, information sharing should be limited.
(3) Before accepting a friend request, one should completely check the profile of the requester. One can make different groups for sharing different kinds of information like a different group for colleagues and family.
(4) Before posting any information on the profile, employees should know their company's policy over sharing any content online on social networks.

For discussion forums

(1) One should pay attention while clicking on links given by various authors. It may be some suspicious site trying to get the credentials of the user.
(2) Users should always keep an eye on the site's URL. Noxious sites may look compellingly indistinguishable from a real one, however, the URL may contain slight inconsistencies like the variety in spelling or an alternate domain (e.g., .com versus.net) [129].
(3) Be careful about communications that requests the client to act promptly, offers something that sounds unrealistic or requests personal information.

Open research issues and challenges

Scientists and researchers have found many methods and solutions to secure users on social media but there are still some issues which are not resolved. In this section, we discuss some of those issues and challenges.

(1) Unfortunately, social networking sites are the easiest way for an attacker to lie about his identity and target the victim. They can lie about their age, looks, and can project themselves as a completely different identity according to their target. Child predators are taking advantage of this drawback in social networking sites, as children are a very easy target on these social platforms. These platforms have millions of users and monitoring each user can be very difficult. Therefore, there is a need for some system which can detect child predators effectively. Although the research community is trying to solve this issue, we need a good and effective system which can stop cyber grooming more efficiently. One possible addition to the already existing systems would be to incorporate artificial intelligence. The chat system can be improved to analyze conversations and derive meaningful inferences to support decision-making.
(2) Social networking sites make money by allowing other companies to show advertisements on their website. Every time a user clicks an advertisement, it takes the user to a page where the user can buy a product and the social networking site get a percentage of that sale. These sites collect data of the users each time they use them so that they can show the advertisements as per the user's interest. In this way, these social networking sites are collecting a huge amount of personal data of

the user which can be sold to hundreds of businesses without user's knowledge. Hence, the user's personal data is at risk. One possible way to thwart such data leaks is to inform the user of the data being shared. This would involve non-technical aspects to enforce a law or contract that all advertisements should abide by. From a technical standpoint there is not much control as to what the parent site decides to share with the advertising agency. Client-side browser restrictions could also provide wrapper-level security.

(3) Nowadays surveys and games are becoming very popular on social media [130]. Generally, these surveys involve entering credentials which are supposed to enable the data for the survey to be gathered or the results to be shared. And while these surveys are collecting credentials, adversaries can skim those details to compromise user's account.

(4) Due to character count limitations on Twitter, people use shortened URLs to share their multimedia content. Adversaries can easily obfuscate malicious sites on these shortened URLs. This is an alarming situation since other social media applications like WhatsApp also have users who have started sharing shortened URLs. However, some social networking sites are working on this issue and have given solutions, but it is as yet conceivable that URL redirection can be used to hop from a safe landing point to a risky landing point. Again, a central repository of phishing sites could be leveraged by the client browser to warn the user when landing on the suspicious website. Further research could be conducted towards preemptive solutions that can parse URLs and warn the user even before clicking. A system is needed which can detect the malicious site from the shortened URLs effectively leveraging the already existing solutions.

(5) Business-oriented networks contain significant business data that can be utilized to perform social engineering attacks. Some LinkedIn invitation update messages have been referred to be utilized as URL redirectors which can divert clients to some vindictive pages. This issue should be resolved so that users can be protected from a targeted attack. Here, intelligent language parsers could be trained to detect sensitive information and warn the originator of the information. Content detection can be applied to such platforms to find malicious activity. It can detect the number of posts posted through a profile because generally, the adversary posts similar messages.

(6) There is a need to secure users on discussion forums also. Users can be easily fooled on discussion forums through phishing attacks which could result in deteriorating user trust on these forums. URL detection and filtering can be applied for these forums also to protect a user from malicious activity. Although such scenarios usually inform the user that they are moving out of the parent domain. The cost to reward ratio here is poor for any forum to implement parsers to parse external links. An incentive-based solution can be thought of to reward sites that scan external links.

Conclusion

Online social networks have become a vital part of the vast internet penetrated world. The paradigm shift has enabled social networks to engage with users on a daily basis. The increased rate of social media usage has solicited the need to make its users aware of the pitfalls, threats, attacks, and privacy issues in them. With the advancement in technology, social media has taken various forms. Individuals can connect to each other in a myriad of ways. Through professional sites, discussion forums, multimedia sharing networks, and many more, netizens can find themselves at the pinnacle of connectivity. Unfortunately, lack of awareness among users regarding security and privacy has the potential to lead to various cyber-attacks through social media. Although academia has come up with innovative solutions to address the security measures that are concerned with social media security, they suffer from a lack of real-world implementation and feasibility. Thus, there is a compelling need to continuously and iteratively review security issues in social networks keeping in pace with technological advancement. In this paper, we presented different scenarios related to online social network threats and their solutions using different models, frameworks, and encryption techniques that protect the social network users against various attacks. We have outlined different solutions and comparative analysis of different survey for better clarity about our survey. However, many of these privacy issues are not yet resolved. In addition to the defensive solutions, parents must monitor the kids actively when they are using internet services like OSNs. Overall, researchers can play a significant role in the defensive approach against these attacks in OSNs but still, some issues need to be resolved by using some hybrid approach, framework, and threat detection tools.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Benson V, Saridakis G, Tennakoon H, Ezingeard JN (2015) The role of security notices and online consumer behaviour: an empirical study of social networking users. Int J Hum Comput Stud 80:36–44
2. Fosso Wamba S, Akter S (2016) Impact of perceived connectivity on intention to use social media: modelling the moderation effects of perceived risk and security. pp 219–227
3. Sahoo SR, Gupta BB (2020) Fake profile detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3):303–331
4. Bailey M, Cooke E, Jahanian F, Xu Y, Karir M A survey of botnet technology and defenses
5. Ahmed M, Mahmood AN, Hu J (2016) A survey of network anomaly detection techniques. J Netw Comput Appl 60:19–31
6. Mislove A, Viswanath B, Gummadi KP, Druschel P (2010) You are who you know. In: Proceedings of the third ACM international conference on Web search and data mining—WSDM '10, p 251
7. Sahoo SR, Gupta BB (2021) Multiple features based approach for automatic fake news detection on social networks using deep learning. Appl Soft Comput 100:106983
8. Jain AK, Gupta BB (2018) Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417
9. Number of social media users worldwide 2010–2021 | Statista [Online]. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. Accessed 14 Dec 2020
10. Gupta BB, Sahoo SR (2021) Online social networks security: principles, algorithm, applications, and perspectives. CRC Press
11. Top 15 Most Popular Social Networking Sites and Apps [August 2018] @DreamGrow [Online]. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/. Accessed 14 Dec 2020
12. Digital Marketing Consultants—SEO Consulting—Zephoria Inc. [Online]. https://zephoria.com/. Accessed 13 Dec 2020
13. Internet Live Stats—Internet Usage &amp; Social Media Statistics [Online]. http://www.internetlivestats.com/. Accessed 14 Dec 2020
14. Data breach causes worldwide 2016 | Statistic [Online]. https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/. Accessed 22 Jan 2021
15. Heimdal Security—Proactive Cyber Security Software [Online]. https://heimdalsecurity.com/en/. Accessed 13 Dec 2018
16. Aggarwal A, Rajadesingan A, Kumaraguru P (2012) PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime pp 1–12
17. Rathore S, Loia V, Park JH (2018) SpamSpotter: an efficient spammer detection framework based on intelligent decision support system on facebook. Appl Soft Comput 67:920–932
18. Michalopoulos D, Mavridis I, Jankovic M (2014) GARS: Real-time system for identification, assessment and control of cyber grooming attacks. Comput Secur 42:177–190
19. Balduzzi M, Egele M, Kirda E, Balzarotti D, Kruegel C (2010) A solution for the automated detection of clickjacking attacks. Asiaccs 4(2):135
20. Sahoo SR, Gupta BB (2020) Popularity-based detection of malicious content in facebook using machine learning approach. In: First international conference on sustainable technologies for computational intelligence. Springer, Singapore, pp 163–176
21. Al-Qurishi M et al (2018) SybilTrap: a graph-based semi-supervised Sybil defense scheme for online social networks. Concurr Comput 30(5):1–10
22. Xu W, Zhang F, Zhu S (2010) Toward worm detection in online social networks. In: Annu. Comput. Secur. Appl. Conf., pp 11–20
23. Biggest online data breaches worldwide 2018 | Statistic [Online]. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/. Accessed 2 Feb2019
24. Facebook to contact 87 million users affected by data breach | Technology | The Guardian [Online]. https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach. Accessed 22 Jan 2021
25. MySpace becomes every hackers' space with top breach in 2016, report says | CSO Online [Online]. https://www.csoonline.com/article/3166846/data-breach/myspace-becomes-every-hackers-space-with-top-breach-in-2016-report-says.html. Accessed 22 Jan 2021
26. FriendFinder Networks hack reportedly exposed over 412 million accounts | TechCrunch [Online]. https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/. Accessed 22 Jan 2021
27. SR Sahoo, BB Gupta (2018) Security issues and challenges in online social networks (OSNs) based on user perspective. In: Computer and cyber security, pp 591–606
28. The Positive Impact of Social Networking Sites on Society [Online]. https://www.makeuseof.com/tag/positive-impact-social-networking-sites-society-opinion/. Accessed 24 Jan 2019
29. Nyaribo YM, Munene AG (2018) Effect of social media pertication in the workplace on employee productivity. IJAME
30. de Vries L, Gensler S, Leeflang PSH (2012) Popularity of brand posts on brand fan pages: an investigation of the effects of social media marketing. J Interact Mark 26(2):83–91
31. Colicev A, Malshe A, Pauwels K, O'Connor P (2018) Improving consumer mindset metrics and shareholder value through social media: the different roles of owned and earned media. J Mark 82(1):37–56
32. Liu F, Xu D (2018) Social roles and consequences in using social media in disasters: a structurational perspective. Inf Syst Front 20(4):693–711
33. The Positive and Negative Effects of Social Networking | Techwalla.com [Online]. https://www.techwalla.com/articles/the-positive-and-negative-effects-of-social-networking. Accessed 23 Jan 2021
34. 7 Negative Effects of Social Media on People and Users [Online]. https://www.makeuseof.com/tag/negative-effects-social-media/. Accessed 24 Jan 2021
35. Rook KS (1984) The negative side of social interaction: impact on psychological well-being. J Pers Soc Psychol 46(5):1097–1108
36. Zhu Y, Xu B, Shi X, Wang Y (2013) A survey of social-based routing in delay tolerant networks: positive and negative social effects. IEEE Commun Surv Tutorials 15(1):387–401
37. Rook KS (2015) Social networks in later life. Curr Dir Psychol Sci 24(1):45–51
38. Wolniewicz CA, Tiamiyu MF, Weeks JW, Elhai JD (2018) Problematic smartphone use and relations with negative affect, fear of missing out, and fear of negative and positive evaluation. Psychiatry Res 262:618–623
39. Faris H et al (2019) An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks. Inf Fusion 48:67–83
40. Bhat SY, Abulaish M (2013) Community-based features for identifying spammers in online social networks. In: Proceedings of the 2013 IEEE/ACM international conference on advances in social networks analysis and mining—ASONAM '13, pp 100–107

41. Whang JJ, Jeong YS, Dhillon IS, Kang S, Lee J (2018) Fast Asynchronous Anti-TrustRank for Web Spam Detection
42. Grosse K, Papernot N, Manoharan P, Backes M, McDaniel P (2017) Adversarial examples for malware detection. Springer, Cham, pp 62–79
43. Kayes I, Iamnitchi A (2017) Privacy and security in online social networks: a survey. Online Soc Netw Media 3–4:1–21
44. Zhang Z, Gupta BB (2018) Social media security and trustworthiness: overview and new direction. Futur Gener Comput Syst 86:914–925
45. Fire M, Goldschmidt R, Elovici Y (2014) Online social networks: threats and solutions. IEEE Commun Surv Tutorials 16(4):2019–2036
46. Chen J, Mishler S, Hu B, Li N, Proctor RW (2018) The description-experience gap in the effect of warning reliability on user trust and performance in a phishing-detection context. Int J Hum Comput Stud 119:35–47
47. Jakobsson M (2018) Two-factor inauthentication—the rise in SMS phishing attacks. Comput Fraud Secur 2018(6):6–8
48. What is identity theft?—Definition from WhatIs.com.[Online]. Available: https://searchsecurity.techtarget.com/definition/identity-theft. Accessed 14 Dec 2018
49. Jain AK, Gupta BB (2021) A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, pp 1–39
50. Identity Theft: The Various Types and Solutions [Online]. https://www.forbes.com/identity-theft/id-theft-and-types.html. Accessed 15 Dec 2020
51. Chaudhary P, Gupta BB (2018) Plague of cross-site scripting on web applications: a review, taxonomy and challenges. Int J Web Based Communit 14(1):64
52. Steffens M, Rossow C, Johns M, Stock B Don't trust the locals: investigating the prevalence of persistent client-side cross-site scripting in the wild
53. Bukhari SN, Ahmad Dar M, Iqbal U (2018) Reducing attack surface corresponding to Type 1 cross-site scripting attacks using secure development life cycle practices. In 2018 fourth international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB), pp 1–4
54. Kaubiyal J, Jain AK (2019) A feature based approach to detect fake profiles in Twitter. In: Proceedings of the 3rd international conference on big data and internet of things, pp 135–139
55. Facebook - Social Media Security | Protecting from Security Threats on Social Media: Facebook, LinkedIn, Twitter and Google Plus - Data Threat Detection and Prevention | Sophos Security Topics - Virus, Malware, Web, Antivirus and Social Media Security Trends [Online]. https://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/facebook.aspx. Accessed 2 Jan 2019
56. Bilge L, Strufe T, Balzarotti D, Kirda E (2009) All your contacts are belong to us. In: Proceedings of the 18th international conference on World wide web—WWW '09, p 551
57. Kaur R, Singh S, Kumar H (2018) Rise of spam and compromised accounts in online social networks: a state-of-the-art review of different combating approaches. J Netw Comput Appl 112:53–88
58. Xin Y, Zhao C, Zhu H, Gao M (2018) A Survey of Malicious Accounts Detection in Large-Scale Online Social Networks. In: 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), pp 155–158
59. Sathish MMK, Indrani B (2018) A study on web hijacking techniques and browser attacks
60. Gao H, Hu J, Huang T (2011) Security issues in online social networks. In: IEEE Internet Comput, pp 56–63
61. Zhang W, Lin Y, Wu J, Zhou T (2018) Inference attack-resistant e-healthcare cloud system with fine-grained access control. In: IEEE Trans. Serv. Comput, pp 1–1
62. Mei B, Xiao Y, Li R, Li H, Cheng X, Sun Y (2018) Image and attribute based convolutional neural network inference attacks in social networks. In: IEEE Trans. Netw. Sci. Eng., pp 1–1
63. Jan MA, Nanda P, He X, Liu RP (2018) A Sybil attack detection scheme for a forest wildfire monitoring application. Futur Gener Comput Syst 80:613–626
64. Mishra AK, Tripathy AK, Puthal D, Yang LT (2019) Analytical model for sybil attack phases in internet of things. IEEE Internet Things J 6(1):379–387
65. Sinha R, Uppal D, Rathi R, Kanwar K (2018) Combating clickjacking using content security policy and aspect oriented programming. Springer, Singapore, pp 323–331
66. Albladi SM, Weir GRS (2018) A semi-automated security advisory system to resist cyber-attack in social networks. Springer, Cham, pp 146–156
67. Clickjacking - OWASP [Online]. https://www.owasp.org/index.php/Clickjacking. Accessed 14 Dec 2018
68. Protecting Your Users Against Clickjacking [Online]. https://www.hacksplaining.com/prevention/click-jacking. Accessed 15 Dec 2018
69. Tian W, Mao J, Jiang J, He Z, Zhou Z, Liu J (2018) Deeply understanding structure-based social network de-anonymization. Procedia Comput Sci 129:52–58
70. Mao J, Tian W, Jiang J, He Z, Zhou Z, Liu J (2018) Understanding structure-based social network de-anonymization techniques via empirical analysis. EURASIP J Wirel Commun Netw 2018(1):279
71. Jiang H et al (2017) SA framework based de-anonymization of social networks
72. Wondracek G, Holz T, Kirda E, Kruegel C (2010) A practical attack to de-anonymize social network users. Proc.—IEEE Symp. Secur. Priv., no. January, pp 223–238
73. What is Cyber Espionage? | Cyber Espionage Definition | Carbon Black [Online]. https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/. Accessed 15 Dec 2018
74. Ghalaty NF, Ben Salem M (2018) A Hierarchical Framework to Detect Targeted Attacks using Deep Neural Network. In: 2018 IEEE International Conference on Big Data (Big Data), pp 5021–5026
75. 5 Crucial Ways To Neutralize Cyber-Espionage [Online]. https://tech.co/5-crucial-ways-neutralize-cyber-espionage-2015-09. Accessed 15 Dec 2018
76. Baldry AC, Sorrentino A, Farrington DP (2018) Post-traumatic stress symptoms among Italian preadolescents involved in school and cyber bullying and victimization. J Child Fam Stud pp 1–7
77. Holfeld B, Mishna F (2018) Longitudinal associations in youth involvement as victimized, bullying, or witnessing cyberbullying . Cyberpsychol Behav Soc Netw 21(4):234–239
78. What is Cyberbullying?—Definition from Techopedia [Online] https://www.techopedia.com/definition/2389/cyberbullying. Accessed 14 Dec 2018
79. What Is Cyberbullying | StopBullying.gov [Online] https://www.stopbullying.gov/cyberbullying/what-is-it/index.html. Accessed 15 Dec 2018
80. Smith PK, Mahdavi J, Carvalho M, Fisher S, Russell S, Tippett N (2008) Cyberbullying: its nature and impact in secondary school pupils. J Child Psychol Psychiatry 49(4):376–385
81. Ngejane C, Mabuza-Hocquet G, Eloff JH, Lefophane S (2018) Mitigating online sexual grooming cybercrime on social media using machine learning: a desktop survey. In 2018 international

conference on advances in Big Data, computing and data communication systems (icABCD) pp 1–6
82. de Santisteban P, del Hoyo J, Alcázar-Córcoles MÁ, Gámez-Guadix M (2018) Progression, maintenance, and feedback of online child sexual grooming: a qualitative analysis of online predators. Child Abuse Negl 80:203–215
83. Internet Safety 101: Grooming [Online]. https://internetsafety101.org/grooming. Accessed 15 Dec 2018
84. Sahoo SR, Gupta BB (2019) Classification of various attacks and their defence mechanism in online social networks: a survey. Enterp Inf Syst 13(6):832–864
85. Cyberstalking | Get Safe Online [Online]. https://www.getsafeonline.org/protecting-yourself/cyberstalking/. Accessed 15 Dec 2018
86. How To Protect Yourself From Cyberstalkers [Online]. https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html. Accessed 15 Dec 2018
87. How to avoid becoming a cyberstalking victim | Association for Progressive Communications [Online]. https://www.apc.org/en/pubs/issue/how-avoid-becoming-cyberstalking-victim. Accessed 15 Dec 2018
88. What is Social Media Security | ZeroFOX. [Online]. https://www.zerofox.com/social-media-security/. Accessed 3 Jan 2019
89. What is Digital Risk Monitoring? [Online]. https://www.zerofox.com/blog/what-is-digital-risk-monitoring/. Accessed 8 Jan 2019
90. Sahoo SR, Gupta BB (2019) Hybrid approach for detection of malicious profiles in twitter. Comput Electr Eng 76:65–81
91. Dinakar K, Picard R, Lieberman H (2015) Common sense reasoning for detection, prevention, and mitigation of cyberbullying. IJCAI Int Jt Conf Artif Intell 3:4168–4172
92. Srinandhini B, Sheeba JI (2015) Online social network bullying detection using intelligence techniques. Procedia Comput Sci 45:485–492
93. Van Royen K, Poels K, Daelemans W, Vandebosch H (2014) Automatic monitoring of cyberbullying on social networking sites: from technological feasibility to desirability. Telemat Inform 32(1):89–97
94. Reynolds K, Kontostathis A, Edwards L (2011) Using machine learning to detect cyberbullying. Proc.—10th Int. Conf. Mach. Learn. Appl. ICMLA, vol 2, pp 241–244
95. Escalante HJ, Villatoro-Tello E, Garza SE, López-Monroy AP, Montes-y-Gómez M, Villaseñor-Pineda L (2017) Early detection of deception and aggressiveness using profile-based representations. Expert Syst Appl 89:99–111
96. Anas A, Khatab S, Salah A (2018) Hovering Patterns: Clickjacking Defense Technique, vol 18, no. 2, pp 130–137
97. Rydstedt G, Bursztein E, Boneh D, Jackson C (2010) Busting frame busting: a study of clickjacking vulnerabilities on popular sites. In: IEEE Oakl. Web 2.0 Secur. Priv. Work., p 6
98. Eterovic-Soric B, Choo KKR, Ashman H, Mubarak S (2017) Stalking the stalkers—detecting and deterring stalking behaviours using technology: a review. Comput Secur 70:278–289
99. Frommholz I, Al-Khateeb HM, Potthast M, Ghasem Z, Shukla M, Short E (2016) On textual analysis and machine learning for cyberstalking detection. Datenbank-Spektrum 16(2):127–135
100. Bendovschi A (2015) Cyber-attacks—trends, patterns and security countermeasures. Procedia Econ Financ 28(April):24–31
101. Ramalingam D, Chinnaiah V (2018) Fake profile detection techniques in large-scale online social networks: a comprehensive review. Comput Electr Eng 65(3):165–177
102. Khan RU, Zhang X, Kumar R, Sharif A, Golilarz NA, Alazab M (2019) An adaptive multi-layer botnet detection technique using machine learning classifiers. Appl Sci 9(11):2375
103. Hakak S, Alazab M, Khan S, Gadekallu TR, Maddikunta PKR, Khan WZ (2021) An ensemble machine learning approach through effective feature extraction to classify fake news. Futur Gener Comput Syst 117:47–58
104. Numan M, Subhan F, Khan WZ, Hakak S, Haider S, Reddy GT, Jolfaei A, Alazab M (2020) A systematic review on clone node detection in static wireless sensor networks. IEEE Access 8:65450–65461
105. Al-Qurishi M, Alrubaian M, Rahman SMM, Alamri A, Hassan MM (2018) A prediction system of Sybil attack in social network using deep-regression model. Futur Gener Comput Syst 87:743–753
106. Faghani MR, Saidi H (2009) Malware propagation in online social networks. In: 2009 4th Int. Conf. Malicious Unwanted Software, MALWARE, pp 8–14
107. Mostafi S, Khan F, Chakrabarty A, Suh DY, Piran MJ (2019) An algorithm for mapping a traffic domain into a complex network: a social internet of things approach. IEEE Access 7:40925–40940
108. Borrego C, Amadeo M, Molinaro A, Jhaveri RH (2019) Privacy-preserving forwarding using homomorphic encryption for information-centric wireless Ad hoc networks. IEEE Commun Lett 23(10):1708–1711
109. Rathee G, Garg S, Kaddoum G, Jayakody DNK, Piran J, Muhammad G (2020) A trusted social network using hypothetical mathematical model and decision-based scheme. IEEE Access
110. Pandey B, Bhanodia PK, Khamparia A, Pandey DK (2019) A comprehensive survey of edge prediction in social networks: techniques, parameters and challenges. Expert Syst Appl 124:164–181. https://doi.org/10.1016/j.eswa.2019.01.040
111. Peng S, Zhou Y, Cao L, Yu S, Niu J, Jia W (2018) Influence analysis in social networks: a survey. J Netw Comput Appl 106:17–32. https://doi.org/10.1016/j.jnca.2018.01.005
112. Dakiche N, Tayeb FBS, Slimani Y, Benatchba K (2019) Tracking community evolution in social networks: a survey. Inf Process Manage 56(3):1084–1102
113. De Salve A, Mori P, Ricci L (2018) A survey on privacy in decentralized online social networks. Comput Sci Rev 27:154–176. https://doi.org/10.1016/j.cosrev.2018.01.001
114. Ramalingam D, Chinnaiah V (2018) Fake profile detection techniques in large-scale online social networks: a comprehensive review. Comput Electr Eng 65:165–177. https://doi.org/10.1016/j.compeleceng.2017.05.020
115. Sarmah U, Bhattacharyya DK, Kalita JK (2018) A survey of detection methods for XSS attacks. J Netw Comput Appl 118:113–143. https://doi.org/10.1016/j.jnca.2018.06.004
116. Song J, Jamous N, Turowski K (2019) A dynamic perspective: local interactions driving the spread of social networks. Enterp Inf Syst 13(2):219–235. https://doi.org/10.1080/17517575.2018.1499133
117. Maleszka M (2018) Application of collective knowledge diffusion in a social network environment. Enterp Inf Syst 1–23
118. Tse YK, Loh H, Ding J, Zhang M (2018) An investigation of social media data during a product recall scandal. Enterp Inf Syst 12(6):733–751. https://doi.org/10.1080/17517575.2018.1455110
119. 10 Tips to Stay Safe on Social Media - Information Technology Services [Online]. https://carleton.ca/its/2016/social-media-safety/. Accessed 14 Dec 2018
120. Foroughi F, Luksch P (2018) Observation measures to profile user security behaviour. In: 2018 International conference on cyber security and protection of digital services (Cyber Security), pp 1–6
121. Thakur K, Hayajneh T, Tseng J (2019) Cyber security in social media: challenges and the way forward. IT Prof 21(2):41–49
122. Harden BJ, Dowd KL, Webb MB, Landsverk J, Testa M (2010) Child welfare and child well-being: new perspectives from the national survey of child and adolescent well-being. Child Welf.

Child Well-Being New Perspect. From Natl. Surv. Child Adolesc. Well-Being, vol 421, pp 1–448

123. Sahoo SR, Gupta BB (2020) Real-time detection of fake account in twitter using machine-learning approach. In: Advances in computational intelligence and communication technology. Springer, Singapore, pp 149–159
124. 8 Social Media Security Tips to Mitigate Risks [Online]. https://blog.hootsuite.com/social-media-security-for-business/. Accessed 14 Dec 2018
125. Byrne E, Vessey JA, Pfeifer L (2018) Cyberbullying and social media: information and interventions for school nurses working with victims, students, and families. J Sch Nurs 34(1):38–50
126. Security Weak Points: Social Media | SolarWinds MSP [Online]. https://www.solarwindsmsp.com/blog/security-weak-points-social-media. Accessed 13 Jan 2019
127. Social Media Security - Security News - Trend Micro USA [Online]. https://www.trendmicro.com/vinfo/us/security/news/social-media-security. Accessed 13 Jan 2019
128. 12 tips for safe social networking | Network World [Online]. https://www.networkworld.com/article/2346606/microsoft-subnet/microsoft-subnet-12-tips-for-safe-social-networking.html. Accessed 13 Jan 2019
129. Social Media - Stay Safe Online [Online]. https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/. Accessed 7 Jan 2019
130. Security Weak Points: Social Media | SolarWinds MSP [Online]. https://www.solarwindsmsp.com/blog/security-weak-points-social-media. Accessed 19 Jan 2019

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.